	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments
1	BRS	L1	18977	((message$1 or data) near3 authenticat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 11:56	
2	BRS	L2	3101	l1 and ((authenticat$3 adj tag) or MAC or "message authentication code")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:00	REv'd images
3	BRS	L3	34	l2 and (((data or input) adj block$1) with random$7)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:57	Rev'd kwic/images
4	BRS	L4	5	l3 and @ad<"20000331"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:08	Rev'd kwic/images
5.	BRS	L5	29	l3 not l4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:09	REv' kwic/images

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments
6	BRS	L6	37	l2 and (((data or input or message) adj block$1) with random$7)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:49	REv'd kwic/images
7	BRS	L7	3	16 not l3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:54	Rev'd kwic/images
8	BRS	L8	3	("5673318", "5757913").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:54	REv'd images
9	BRS	L10	2	l9 and (((data or input) adj block$1) with random$7)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:57	REv'd kwic/images
10	BRS	L9	13	l2 and (block adj (identifier$1 or index$2))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 12:57	REv'd kwic/images

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments
13	BRS	L13	38	12 and (.((data or input or message) adj block$1) with $7random$7)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	2005/06/06 15:05	Rev'd kwic/images

```
message authentication code CBC-MAC XOR-MAC block
identifier block index
```

Web ⯆ > all ⯆

search   clear

Feeling Lucky

Exact Phrase:

Any of the Words:

Without the Words:

Results only ⯆ from the domain

File Format: only ⯆

all ⯆

Occurrence: anywhere in the page ⯆ **Date**

○ in the last: (anytime) ⯆

◉ between:

March ⯆ 31 ⯆ 2000 ⯆

◉

and

○

January ⯆ 1 ⯆ 2004 ⯆

Open results in: this window ⯆

Duplicates Filter: on ⯆

Safesearch: Off ⯆

Results: 10 ⯆

Country: all ⯆

Language: all ⯆

Keyboard: à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ø ù ú û ü ý þ

The Google Ultimate Interface - from the creator of Fagan Finder
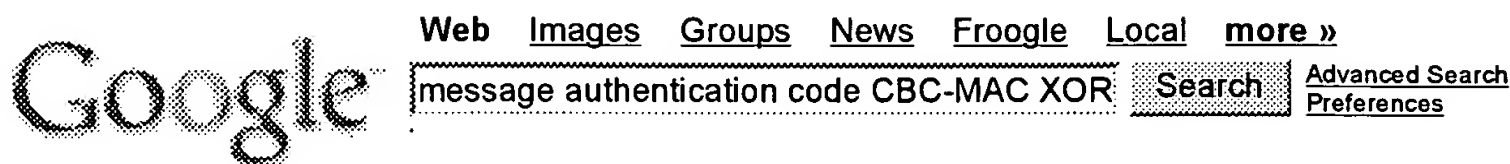
>> make this my homepage <<   This site is not endorsed by Google.

Like this tool? See also:

Fagan Finder, Translation Wizard, URLinfo, Speed Browse, All About RSS, and Blog Search Engines.

Google   message authentication code CBC-MAC XOR   Search   Advanced Search
Preferences

Web Results **1 - 10** of about **13** for **message authentication code CBC-MAC XOR-MAC block identifier bloc**

tripwire-2.3.1.2.orig/man/man4/.cvsignore +++ tripwire-2.3.1.2/man ...
All classes derived from BlockTransformation are **block** ciphers in ECB mode (for
example ... abstract base class for **message authentication** codes +//! add to ...
debian.fapeal.br/debian-non-US/pool/ non-US/main/t/tripwire/tripwire_2.3.1.2-6.1.diff - 513k -
Cached - Similar pages

[PS] Introduction to Modern Cryptography Mihir Bellare 1 Phillip ...
File Format: Adobe PostScript - View as Text
The **CBC MAC** uses the **block** cipher E to generate an n-bit MAC for messages whose
lengths are some multiple of ... **block** chaining **message authentication code**. ...
www.cs.ucdavis.edu/~rogaway/ classes/227/fall01/book/main.ps - Similar pages

[PS] This is a Chapter from the Handbook of Applied Cryptography, by A ...
File Format: Adobe PostScript - View as Text
see also **Block** cipher see also Public-key encryption see also Stream cipher ...
existential; 326 selective, 326 see also **CBC-MAC Message authentication** tag ...
www.cacr.math.uwaterloo.ca/hac/about/**index**.ps - Similar pages

[PDF] This is a Chapter from the Handbook of Applied Cryptography, by A ...
File Format: PDF/Adobe Acrobat - View as HTML
Key **authentication**, 492. Key clustering attack on **block** ciphers, 281 ... see also
CBC-MAC. Message authentication tag system, 376. **Message** Authenticator ...
www.cacr.math.uwaterloo.ca/hac/about/**index**.pdf - Similar pages

[PDF] MDiCE R1.1
File Format: PDF/Adobe Acrobat - View as HTML
Weitere **Block** cipher: IDEA, DES, Triple DES (DES-EDE2 and ... **Message authentication**
codes: MD5-MAC, HMAC, **XOR-MAC**,. **CBC-MAC**, DMAC ...
www.fh-kaernten.at/mdice/download/ MDiCE_Technische_Dokumentation.pdf - Similar pages

digital certificate mumbai
Bitzer's hash function, 374 plaintext-ciphertext **block** chaining Black-box, 329,
341, 369, ... MAC, see **Message authentication code** (MAC) security of, 465 ...
services.eliteral.com/ digital-certificate-mumbai/cryptography.php - 132k - Cached - Similar pages

digital certificate mumbai
9.7 Definition A **message authentication code** (MAC) algorithm is a family of ...
9.58 Algorithm **CBC-MAC** INPUT: data x; specification of **block** cipher E; ...
services.eliteral.com/ digital-certificate-mumbai/chap9.php - 267k - Cached - Similar pages

SSL/TLS Terms and Acronyms (Including Some General Cryptography ...
CBC-MAC: Cipher **Block** Chaining **Message Authentication Code**; CDMF: Commercial Data
Masking Facility ... **XOR-MAC**: Exclusive OR **Message Authentication Code**. ...
www.technoids.org/tlsglossary.html - 27k - Cached - Similar pages

[PS] Lecture Notes on Cryptography Shafi Goldwasser 1 Mihir Bellare 2 ...
File Format: Adobe PostScript - View as Text
8.6 The **CBC MAC** The most popular **message authentication code** in use is the CBC
... The security of the cipher **block** chaining **message authentication. code**. ...

www.cs.ucsd.edu/users/mihir/papers/gb.ps - <u>Similar pages</u>

[PDF] <u>Cryptographic Primitives for Information **Authentication** — State of ...</u>
File Format: PDF/Adobe Acrobat
for the Output FeedBack (OFB) mode of any **block** cipher. **...** plaintext P with an
authenticator, **Message Authentication Code**, or MAC. The **...**
www.springerlink.com/**index**/1N4AWPVBR011DN6P.pdf - <u>Similar pages</u>

Google ▶

Result Page: **1** <u>2</u>   **<u>Next</u>**

Free! Get the Google Toolbar. <u>Download Now</u> - <u>About Toolbar</u>

Google ▾ [   ] ▾ G Search ▾ ⟋ 🖸 277 blocked ⚐ Check ▾ ⟍ AutoLink ▾ 🗌 AutoFill

[message authentication code CBC-M] Search

<u>Search within results</u> | <u>Language Tools</u> | <u>Search Tips</u> | <u>Dissatisfied? Help us improve</u>

<u>Google Home</u> - <u>Advertising Programs</u> - <u>Business Solutions</u> - <u>About Google</u>

©2005 Google